COOLEY LLP
MICHAEL G. RHODES (116127) (rhodesmg@cooley.com)
MATTHEW D. BROWN (196972) (brownmd@cooley.com)
BENJAMIN H. KLEINE (257225) (bkleine@cooley.com)
RITESH SRIVASTAVA (246477) (rsrivastava@cooley.com)
101 California Street, 5th Floor
San Francisco, CA 94111-5800
Telephone: (415) 693-2000
Facsimile: (415) 693-2222

Attorneys for Defendant LinkedIn Corporation

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

IN RE LINKEDIN USER PRIVACY LITIGATION

Case No. 12-CV-3088 EJD

DEFENDANT LINKEDIN CORPORATION'S MOTION TO DISMISS PLAINTIFFS' FIRST AMENDED CONSOLIDATED CLASS ACTION COMPLAINT

Courtroom: 4 (5th Floor)
Judge: Hon. Edward J. Davila
Date: Feb. 8, 2013
Time: 9:00 a.m.
Trial Date: None Set

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

TABLE OF AUTHORITIES
(continued)

Page(s)

STATUTES

OTHER AUTHORITIES

NOTICE OF MOTION AND MOTION TO DISMISS

TO ALL PARTIES AND THEIR ATTORNEYS OF RECORD:

PLEASE TAKE NOTICE that on February 8, 2013 at 9:00 a.m. or as soon thereafter as this motion may be heard in the above-entitled court, located at 280 South 1st Street, San Jose, California, in Courtroom 4 (5th Floor), Defendant LinkedIn Corporation ("LinkedIn") will move to dismiss Plaintiffs' First Amended Consolidated Class Action Complaint ("First Amended Complaint" or "FAC"). LinkedIn's Motion is made pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6) and is based on this Notice of Motion and Motion, the accompanying Memorandum of Points and Authorities, LinkedIn's Request for Consideration of Documents Incorporated Into the Complaint and for Judicial Notice filed herewith, the Declaration of Eric Heath ("Heath Decl.") and exhibits thereto filed herewith, all pleadings and papers on file in this matter, and such other matters as may be presented to this Court at the time of hearing or otherwise.

STATEMENT OF RELIEF SOUGHT

LinkedIn seeks an order, pursuant to Federal Rules of Civil Procedure 12(b)(1) and 12(b)(6), dismissing with prejudice the First Amended Complaint and each of its causes of action for lack of standing and failure to state a claim upon which relief can be granted.

STATEMENT OF ISSUES TO BE DECIDED

1. Whether Plaintiffs have standing under Article III of the U.S. Constitution.

2. Whether the First Amended Complaint states a claim upon which relief can be granted.

MEMORANDUM OF POINTS AND AUTHORITIES

I. INTRODUCTION

Through this litigation, Plaintiffs seek to capitalize on a criminal intruder's posting of approximately 6.5 million stolen LinkedIn passwords (but not associated email addresses or other member information) on a Russian hacker website. Plaintiffs' core allegation is that although LinkedIn's Privacy Policy states that information provided by members will be protected with industry standard protocols and technology, LinkedIn stored passwords in "unsalted SHA-1

hashed format," a form of encryption that Plaintiffs allege is "outdated." Plaintiffs' First Amended Complaint ("FAC") should be dismissed because, like the predecessor complaint, it is devoid of any allegation that Plaintiffs suffered any injury in fact that would confer standing to pursue their claims in federal court and fails to state a claim as a matter of law.[1]

The FAC should be dismissed under Rule 12(b)(1) for lack of Article III standing because Plaintiffs have still not alleged injury in fact resulting from the use of LinkedIn's encryption method (or, for that matter, any other data security practice). Among other things, Plaintiffs have not alleged that any third party has used stolen passwords to access any of Plaintiffs' personal information. Further, even if a third party somehow could log into Plaintiffs' LinkedIn accounts, Plaintiffs make no allegation that sensitive information such as credit card numbers or social security numbers would be available to the hacker. Moreover, one of the two Plaintiffs, Szpyrka, does not even allege that her password was stolen in the first place. Plaintiffs' allegations constitute nothing more than speculation about hypothetical future harm that is insufficient to establish standing to sue.

Independently, the FAC should be dismissed under Rule 12(b)(6) for failure to state a claim. First, Plaintiffs' Unfair Competition Law (UCL) claim fails because, among other deficiencies, they do not allege injury in fact or lost money or property as result of the alleged unfair competition, nor have they pled their fraud-based claim with particularity. Second, Plaintiffs' breach of contract and implied contract claims fail because they do not allege legal damages; Plaintiffs' claim for "monies paid" to LinkedIn in exchange for additional premium

[1] On November 5, 2012, LinkedIn filed a Motion to Dismiss Plaintiffs' Consolidated Class Action Complaint. (Dkt. 51.) In response, on November 26, 2012, after the deadline to file an opposition to LinkedIn's Motion to Dismiss had passed, Plaintiffs filed the FAC. (Dkt. 54.) In the FAC, Plaintiffs have removed all references to plaintiff Scott Shepherd and have removed the "Data Breach Class" that he purported to represent—a class that consisted of LinkedIn members who had not paid for LinkedIn's "premium services." Plaintiffs have added as a named Plaintiff Khalilah Wright, who, like Plaintiff Katie Szpyrka, is alleged to be another "paying" LinkedIn member who opted to receive "premium services." The FAC thus contains allegations pertaining only to LinkedIn users who have paid for LinkedIn's premium services. Additionally, Plaintiffs have dropped their claim under the Consumer Legal Remedies Act and added claims for "restitution/unjust enrichment."

services is not a claim for contract damages, but is a claim for restitutionary relief that is improper where they do not plead fraud in the inducement or a "total" breach that would justify the remedy of restitution. Third, Plaintiffs' "restitution/unjust enrichment" claims fail because unjust enrichment is not an independent cause of action under California law (nor is restitution, which is a remedy) and, even if it were, the parties do not dispute the validity and existence of the contract between the parties, which is an explicit prerequisite for such a cause of action. Additionally, because Plaintiffs do not allege fraud in the inducement or a "total" breach, they fail to allege any alternative theory for restitution. Fourth, Plaintiffs' claim for breach of the implied covenant of good faith and fair dealing fails because it is duplicative of the breach of contract claims and does not allege conscious and deliberate conduct. Finally, Plaintiffs' negligence and "negligence *per se*" claims fail because there are insufficient allegations of appreciative, non-speculative, present injury; because their claims are barred by the "economic loss rule," which precludes negligence actions based on value or quality deviations that do not result in property damage or personal injury; and because the UCL claim underlying the negligence *per se* claim also fails.

LinkedIn takes all matters relating to its members' privacy and security very seriously. LinkedIn employs world-class security experts, has policies and personnel focused on data security, and implemented a robust, industry-standard security program to protect its members' data, including passwords, at all relevant times. LinkedIn's actions were fully consistent with the Privacy Policy, which it would prove if this case were to proceed past the pleading stage. But at the present stage, because Plaintiffs lack standing to pursue their claims and fail to state a claim upon which relief can be granted, the FAC should be dismissed in its entirety. Moreover, because any further amendment would be futile given the fundamental problems with Plaintiffs' case—despite now having amended their Consolidated Class Action Complaint in response to LinkedIn's first motion to dismiss—the FAC should be dismissed with prejudice.

II. STATEMENT OF FACTS[2]

A. LinkedIn and Its Privacy Policy.

LinkedIn operates the website www.LinkedIn.com, which provides an online community for professional networking. (FAC ¶¶ 2, 12.) LinkedIn is available at no cost to anyone age 18 or older who wants to join. A prospective member registers for an account by providing a name, email address, and password. (*Id.* ¶ 13.) Once registered, a member logs into his or her account by entering the email address the member has designated in combination with a password. A member may create a professional "profile" containing information such as educational and employment history. (*Id.*)

When prospective members register (sign up) for an account, they click a button labeled "Join Now" which confirms that they agree to LinkedIn's User Agreement ("User Agreement") and Privacy Policy ("Privacy Policy"). (*Id.* ¶ 15.) Once registered, members may opt to upgrade their account to a paid "premium" account for a certain monthly fee which provides members with enhanced tools such as premium search features, additional search alerts, and extra folders to manage and save searches. (*Id.* ¶ 14.) Members do not agree to any new User Agreement or Privacy Policy when purchasing upgraded, premium services. Instead, in exchange for the additional services provided by LinkedIn, the upgrading members merely agree to a few new terms related to payment; the remainder of the language is exactly the same as the User Agreement to which they previously agreed when, as prospective members, they initially registered for a LinkedIn account. (*See id.* ¶¶ 15-16; *compare* Heath Decl. Ex. A (User Agreement assented to when initially signing up for free LinkedIn account) *with id.* Ex. C (terms assented to when later upgrading to premium services).)[3]

---

[2] This statement is based on the allegations in the FAC, which LinkedIn does not admit.

[3] Copies of the User Agreement to which prospective members assent during initial registration, the terms to which members later assent when upgrading to premium services, and the Privacy Policy are provided as Exhibits A-C to the concurrently filed Declaration of Eric Heath. The FAC cites and quotes these agreements, which form the basis of Plaintiffs' claims, and therefore they are incorporated by reference into the FAC. (*See* concurrently filed Request for Consideration of Documents Incorporated Into the Complaint and for Judicial Notice.) *See also Tellabs, Inc. v. Makor Issues & Rights, Ltd.*, 551 U.S. 308, 322 (2007) ("[C]ourts must consider the complaint in its entirety . . . in particular, documents incorporated into the complaint by

LinkedIn's Privacy Policy briefly describes how it maintains its members' personal information. While Plaintiffs' FAC quotes only one statement regarding security, the Policy actually provides substantial additional detail on what security measures LinkedIn employs. The Privacy Policy summarizes selected "Highlights" at the top of the page, followed immediately by the full Policy. Highlight number 6 states in part:

> 6. Security
>
> - Personal information you provide will be secured in accordance with industry standards and technology. Since the internet is not a 100% secure environment, we cannot ensure or warrant the security of any information you transmit to LinkedIn. There is no guarantee that information may not be accessed, copied, disclosed, altered, or destroyed by breach of any of our physical, technical, or managerial safeguards.

(Heath Decl. Ex. B.) The "Introduction" to the full Privacy Policy states:

> Of course, maintaining your trust is our top concern, so we adhere to the following principles to protect your privacy:
>
> * * *
>
> - All information that you provide will be protected with industry standard protocols and technology.

(*Id.*) The "industry standard protocols and technology" that LinkedIn agrees to use are later specified in Section 6 of the full Privacy Policy:

> 6. Security
>
> In order to help secure your personal information, access to your data on LinkedIn is password-protected, and sensitive data (such as credit card information) is protected by SSL encryption when it is exchanged between your web browser and the LinkedIn website. To protect any data you store on our servers, LinkedIn also regularly audits its system for possible vulnerabilities and attacks, and we use a tier-one secured-access data center. However, since the internet is not a 100% secure environment, we cannot ensure or warrant the security of any information you transmit to LinkedIn. There is no guarantee that information may not be accessed, disclosed, altered, or destroyed by breach of any of our physical, technical, or managerial safeguards. It is your responsibility to protect the security of your login information. Please note that emails, instant messaging, and similar means of communication

---

reference, and matters of which a court may take judicial notice."); *U.S. v. Ritchie*, 342 F.3d 903, 908 (9th Cir. 2003) (a document is "incorporated by reference into a complaint if the plaintiff refers extensively to the document or the document forms the basis of the plaintiff's claim").

> with other Users of LinkedIn are not encrypted, and we strongly advise you not to communicate any confidential information through these means.

(*Id.*)

B. The Hacking Attack on LinkedIn.

Plaintiffs allege that sometime before June 6, 2012, hackers infiltrated LinkedIn's computer systems. (FAC ¶ 4.) On June 6, 2012, the hackers posted approximately 6.5 million stolen, encrypted passwords online. (*Id.* ¶ 27.) Based on a newspaper story, Plaintiffs make a generalized allegation "on information and belief" that email addresses may also have been taken. (*Id.* ¶ 29 & n.8.) Aside from this, Plaintiffs have not alleged that any information other than passwords was stolen, posted, or used, or that any other member information was improperly secured. (*See id.* ¶ 18 ("In particular, LinkedIn failed to adequately protect user data because it stored passwords in unsalted SHA-1 hashed format."); *id.* ¶ 27.)

At the time, LinkedIn had recently completed a switch of its password encryption method from a system that stored member passwords in a hashed format to one that both salted and hashed passwords, thereby providing a higher level of security.[4] (*Id.* ¶ 31.) However, the encryption technique used by LinkedIn for member passwords did not contribute in any way to the hacker's ability to gain access to LinkedIn's systems. (*Id.* ¶ 21 ("LinkedIn failed to use a modern hashing and salting function, and therefore drastically exacerbated the *consequences* of a hacker bypassing its outer layer of security.") (italics added).) After learning of the attack, LinkedIn sent emails to members whose passwords were stolen. (*Id.* ¶ 49.)

C. Plaintiffs and their Allegations.

Plaintiffs' core allegation is that LinkedIn's Privacy Policy states that "[a]ll information that [they] provide [to LinkedIn] will be protected with industry standard protocols and technology" (*id.* ¶ 3) but that "LinkedIn failed to adequately protect user data because it stored

[4] According to the FAC, "hashing" is a process by which text is inputted into a cryptographic function and converted into an unreadable, encrypted format (FAC ¶ 18 n.3) and "salting" is a process whereby random values are combined with a password before the text is hashed (*id.* ¶ 19).

passwords in unsalted SHA-1 hashed format" (*id.* ¶ 18). Plaintiffs allege that SHA-1 is "an outdated hashing function" and "runs afoul of conventional data protection methods." (*Id.* ¶ 18.)

Plaintiff Khalilah Wright alleges she is a resident of Virginia and a LinkedIn member. (*Id.* ¶ 7.) She alleges that on June 7, 2012, she received an email from LinkedIn about her password being compromised. (*Id.* ¶ 49.) Plaintiff Katie Szpyrka alleges that she is a resident of Illinois and a LinkedIn member. (*Id.* ¶ 6.) In contrast to Wright, she does *not* allege that her LinkedIn password was stolen. Both Plaintiffs allege that they pay LinkedIn for LinkedIn's premium services and that had they known that LinkedIn was not encrypting their password in salted, hashed format, they would have paid less or not at all for those premium services. (*See, e.g., id.* ¶¶ 39, 43, 47, 51.) Plaintiffs also allege that they provided LinkedIn with their personal information and that they would not have done so had they known that passwords were not encrypted in salted, hashed format. (*Id.* ¶¶ 44, 52.)

Notably absent from the FAC is any allegation that any third party has improperly accessed Plaintiffs' LinkedIn accounts as a result of the password theft, that either Plaintiff has suffered any other harm directly resulting from the password theft, or that any such improper access or harm is likely to befall Plaintiffs. Plaintiff Szpyrka, in fact, does not even allege that her password was stolen at all. Furthermore, despite their allegations that it was a material term of the agreement between LinkedIn and Plaintiffs, neither Plaintiff alleges that she actually read the statement in LinkedIn's Privacy Policy that "[p]ersonal information you provide will be secured in accordance with industry standard protocols and technology."

III. APPLICABLE STANDARDS

Unless a plaintiff establishes standing under Article III of the U.S. Constitution, a federal court does not have subject matter jurisdiction to hear the case. *See Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 101-02 (1998). A defendant may challenge standing through a Rule 12(b)(1) motion and may either attack the complaint on its face or the existence of jurisdiction in fact. *See Thornhill Publ'g Co. v. Gen. Tel. & Elecs. Corp.*, 594 F.2d 730, 732-33 (9th Cir. 1979). If a complaint does not establish standing, a federal court must dismiss the case. *See Steel Co.*,

523 U.S. at 101-02. The burden of establishing standing rests on plaintiffs. *Colwell v. Dep't of Health and Human Servs.*, 558 F.3d 1112, 1121 (9th Cir. 2009).

A court must dismiss a complaint under Rule 12(b)(6) where it fails to allege facts sufficient to support a cognizable legal claim. *Shroyer v. New Cingular Wireless Servs., Inc.*, 622 F.3d 1035, 1041 (9th Cir. 2010) (dismissal is proper where "there is no cognizable legal theory or an absence of sufficient facts alleged to support a cognizable legal theory"). As the Supreme Court has emphasized, "[l]abels and conclusions, and a formulaic recitation of the elements of a cause of action will not [survive a motion to dismiss]," and "courts are not bound to accept as true a legal conclusion couched as a factual allegation." *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 555-56 (2007) (internal quotation marks and citation omitted). Instead,

> a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.' A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.

Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009) (citation omitted). Thus, "where the well-pleaded facts do not permit the court to infer more than the mere possibility of misconduct, the complaint has alleged—but it has not show[n]—that the pleader is entitled to relief." *Id.* (internal quotation marks and citation omitted). Furthermore, while a court must accept all well-pleaded factual allegations as true, unwarranted conclusions and inferences need not be accepted. *See Doe I v. Wal-Mart Stores, Inc.*, 572 F.3d 677, 681-83 (9th Cir. 2009) (citing *Twombly* and *Iqbal*).

IV. ARGUMENT

A. Plaintiffs Lack Article III Standing (All Claims).

In order to have standing under Article III to pursue a claim in federal court, a plaintiff bears the burden of alleging "injury in fact," which is "an injury to himself that is 'distinct and palpable' as opposed to merely '[a]bstract,' and the alleged harm must be actual or imminent, not 'conjectural' or 'hypothetical.'" *Whitmore v. Ark.*, 495 U.S. 149, 155 (1990) (citations omitted). Hypothetical future harms do not suffice; instead, only future harms that are "imminent" and "certainly impending" can constitute injury in fact. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 564 n.2 (1992); *Whitmore*, 495 U.S. at 158. Moreover, in a putative class action, the named

plaintiffs must each establish that they personally have standing or they may not seek such relief on behalf of the class. *See Lewis v. Casey*, 518 U.S. 343, 357 (1996) ("[E]ven named plaintiffs who represent a class 'must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent.'") (citations omitted); *Lierboe v. State Farm Mut. Auto. Ins. Co.*, 350 F.3d 1018, 1022-23 (9th Cir. 2003) (same).

Plaintiffs make no allegation that they actually incurred any harm from any misuse of passwords subsequent to the theft, or that any such harm is "imminent" or "certainly impending," and thus the FAC should be dismissed for lack of Article III standing. Plaintiff Szpyrka does not even allege that her password was among those that were stolen, let alone that her password was posted online, that it was decrypted, or that a third party used the password in any way. She therefore has not alleged injury in fact sufficient to establish Article III standing. *See Sierra Club v. Morton*, 405 U.S. 727, 734-35 (1972) (injury in fact test "requires that the party seeking review be himself among the injured").

While Plaintiff Wright does allege that her password was stolen, she does not allege that her password was actually misused by any third party or that she was otherwise harmed by any misuse of her password. Nor does Wright allege that harmful use of her password is "imminent" or "certainly impending." In a consistent line of cases, the Supreme Court has held that plaintiffs do not have standing under Article III where no harm has yet occurred and any alleged future harm is neither "imminent" nor "certainly impending." *See, e.g.*, *Lujan*, 504 U.S. at 564 (plaintiffs did not have standing to enjoin funding of activities that threatened certain species' habitats where plaintiffs had not alleged that they, personally, had visited the habitats in question to see the destruction of wildlife at issue, because plaintiffs' intent to return to the sites in the future did not transform the injury from hypothetical to "imminent"); *City of Los Angeles v. Lyons*, 461 U.S. 95, 105-06 (1983) (plaintiff previously subjected to chokehold technique by police department had no standing to enjoin future use of technique because future injury was not "real and immediate" since it would occur only if the police again arrested him and again used the technique on him). Wright's allegations amount to pure speculation of hypothetical future harm:

some unidentified third party, at some point in the future, *might* use her password to cause her harm. The FAC should therefore be dismissed for lack of standing.[5] *See Whitmore*, 495 U.S. at 158 ("speculative" or "hypothetical" harms do not satisfy Article III).

In the context of data breaches, courts have held that the disclosure of personal information—even social security numbers, credit card numbers, names, telephone numbers, and addresses—does not constitute injury in fact in the absence of specific allegations that the personal information disclosed has been used in a way that harmed plaintiffs or that such use is certainly impending. For example, in a recent decision, the Third Circuit surveyed recent case law on standing in data breach cases and held that the plaintiffs' allegation of hypothetical, future injury from the disclosure of their personal information was insufficient to establish Article III standing. *Reilly v. Ceridian Corp.*, 664 F.3d 38 (3d Cir. 2011). The plaintiffs in *Reilly* were employees of a law firm that had contracted with Ceridian to provide payroll services. In a security breach, a hacker infiltrated Ceridian's computer systems and gained access to the personal and financial information of thousands of employees, *including names, social security numbers, birth dates, and bank account numbers*. *Id.* at 40. The plaintiffs in *Reilly* alleged that the security breach increased the risk that their personal information would be misused or that they would be the subject of identity theft. 664 F.3d at 40. The court held that the plaintiffs' allegations were insufficient to establish injury in fact because "[a]llegations of 'possible future injury' are not sufficient to satisfy Article III." *Id.* at 42 (citing *Whitmore*, 495 U.S. at 158). The

[5] Further, the FAC does not even contain a clear allegation that Wright's password was decrypted. (*See* FAC ¶ 49.) The FAC alleges that *some* members' passwords were decrypted (*see id.* ¶ 27), but nowhere clearly states that Wright's password was among them. Instead, Plaintiffs use carefully crafted wording to allege that LinkedIn's encryption method has made it easier for hackers to decrypt affected members' passwords (including Wright's) while stopping short of actually alleging that Wright's password has, as of yet, been decrypted. (*See id.* ¶¶ 33, 72, 97 (alleging that LinkedIn's failure to use industry standard protocols and technology to protect PII "significantly contributed *to the hacker's ability* to gain access to LinkedIn's network, and to ultimately decipher and disclose Plaintiff Wright's and the Subclass members' PII to the public") (italics added); *id.* ¶ 126 (alleging that if LinkedIn had used industry standard protocols, "it would have been drastically more difficult to decipher Plaintiff Wright's and the Subclass members' passwords").) Plaintiffs therefore seem to want to insinuate that Wright's password was decrypted without stating this definitively. The lack of a clear allegation that Wright's password was decrypted is yet another reason that Wright lacks Article III standing.

plaintiffs' allegations were merely "hypothetical, future injury . . . insufficient to establish standing," because in order to be injured, the plaintiffs would have had to show that "the hacker: (1) read, copied, and understood [the plaintiffs'] personal information; (2) intends to commit future criminal acts by misusing the information; and (3) is able to use such information to the detriment of [the plaintiffs] by making unauthorized transactions in [the plaintiffs'] names." *Reilly*, 664 F.3d at 42. Since the plaintiffs could not allege that any of those things had happened, there was no "certainly impending" harm. *Id.*; *see also Low v. LinkedIn Corp.*, No. 11-cv-1468, 2011 WL 5509848, at *3 (N.D. Cal. Nov. 11, 2011) (finding no particularized harm sufficient to establish Article III standing where "[p]laintiff has not alleged *how* third party advertisers would be able to infer [plaintiff's] personal identity from LinkedIn's anonymous user ID combined with [plaintiff's] browsing history") (emphasis in original).

Like the plaintiffs in *Reilly*, Plaintiffs here have not explicitly alleged that their passwords have been "read . . . and understood"; nor have they alleged that anyone "intends to commit future criminal acts" with their passwords or that anyone is even able to "use [their passwords] to [their] detriment." *See Reilly*, 664 F.3d at 42. But whereas the information stolen in *Reilly* included names, social security numbers, birth dates, and bank account numbers—pieces of information that could possibly be used to inflict actual harm—Plaintiffs here do not allege that any such information was stolen, but instead allege only that passwords and, "on information and belief," "probably" email addresses, were stolen.[6] Additionally, Plaintiffs make no allegation that a third party has already logged into their LinkedIn accounts.[7] It is not surprising, therefore, that

[6] In response to LinkedIn's first Motion to Dismiss, Plaintiffs, in their FAC, now allege, "on information and belief," that email addresses were also taken, because according to a newspaper story, even though only passwords were posted online, "that is *probably* because whoever breached [LinkedIn's] systems simply kept those [user names] for themselves." (FAC ¶ 29 n.8) (italics added).) Even if Plaintiffs' allegation on information and belief that email addresses were "probably" taken were true, that allegation would not solve the FAC's primary deficiency—that Plaintiffs have not alleged that any harm has occurred or is certainly impending. Instead, if email addresses had been stolen and used in combination with passwords—one cannot log into an account without both the password and the corresponding email address designated by the user—Plaintiffs would be expected to have included allegations of such use and the corresponding harm.

[7] Plaintiffs' generalized claim that "*hackers know full well that people tend to use the same password across multiple sites and will test those passwords*" on other accounts (FAC ¶ 28)

in sharp contrast to the plaintiffs in *Reilly*, Plaintiffs here do not make *any* allegation that they are at increased risk of identity theft—let alone that such identity theft has occurred or is certainly impending.[8] Moreover, Plaintiffs make no allegation that sensitive information such as credit card numbers, bank account numbers, or social security numbers would be available in their LinkedIn accounts.[9]

While in some cases courts have held that the loss of personal information may be sufficient to confer Article III standing, those cases involved sensitive personal information that could be used for harm and a credible risk of imminent injury. For example, in *Krottner v. Starbucks Corp.*, 628 F.3d 1139 (9th Cir. 2010), plaintiffs were Starbucks employees who had had their *names, addresses, and social security numbers* stolen as a result of the theft of a company laptop, and plaintiffs alleged that someone had attempted to open a bank account with one plaintiff's stolen information. The Ninth Circuit held that plaintiffs had satisfied the injury in fact requirement through their allegations of increased risk of future identity theft because they had "alleged a credible threat of real and immediate harm stemming from the theft of a laptop containing their unencrypted personal data." *Id.* at 1143. Here, Plaintiffs have not put forward any allegation of how the theft of passwords (and, "probably," email addresses) has caused them harm, imminently will cause them harm, or even *can* cause them harm given that LinkedIn reset users' passwords following discovery of the theft. *See Low*, 2011 WL 5509848, at *6 (holding

---

should be rejected. Not only is this pure conjecture, it also irrelevant to whether *these* Plaintiffs have actually suffered concrete injury. Plaintiffs do not allege that *they* have used the same password across websites and they have not alleged that *they* have had any other online account hacked. So their speculation about what hackers might think or what such hackers hypothetically might be able to do vis-à-vis unnamed people's online accounts says nothing at all about whether *these* Plaintiffs have suffered injury in fact.

[8] The lack of any allegation of increased risk of identity theft is no accident. Plaintiffs had included conclusory allegations of this sort in the earlier Consolidated Class Action Complaint (*see* Consolidated Class Action Complaint ¶ 43 ("Plaintiff Shepherd had his PII compromised, exposing him to a heightened risk of identity theft . . ."); *id.* ¶ 83 (LinkedIn's alleged failure to properly secure members' passwords "exposed Plaintiff Shepherd and the Data Breach Class members to a heightened risk of identity theft . . .")), but they have dropped these allegations from the FAC.

[9] Plaintiffs *cannot* make such an allegation because, in fact, this information is not available on LinkedIn members' account pages.

that, unlike *Krottner*, "Low has not alleged that his credit card number, address, and social security number have been stolen or published or that he is a likely target of identity theft as a result of LinkedIn's practices. Nor has Low alleged that his sensitive personal information has been exposed to the public. Indeed, the Plaintiff has failed to put forward a coherent theory of how his personal information was disclosed or transferred to third parties, and how it has harmed him. Accordingly, Low has failed to allege an injury-in-fact.").

Nor is Article III standing conferred by Plaintiffs' conclusory allegation that they relied on the statement in the Privacy Policy that "[a]ll information that [they] provide [to LinkedIn] will be protected with industry standard protocols and technology." (FAC ¶¶ 3, 15.) Plaintiffs Szpyrka and Wright allege that they relied on this statement when they created their LinkedIn account and when they paid for LinkedIn's premium services. (*Id*. ¶¶ 41, 43, 48, 51.) They allege that, as a result, they "did not receive the benefit of the bargain in that the services provided were worth less than [they] paid for them, and that she paid more than she otherwise would have based upon [LinkedIn's] User Agreement and Privacy Policy." (*Id*. ¶¶ 43, 51.) Plaintiffs also allege that they "paid" for LinkedIn's services by providing LinkedIn with their "Personally Identifiable Information" and that "[h]ad [they] known of [LinkedIn's] substandard security procedures and methods of protecting and storing [their] PII, [they] would not have provided [their] personal and confidential information in exchange for access to Defendant's services." (*Id*. ¶¶ 44, 52.) They allege that they "did not receive the benefit of the bargain in that the services provided were not commensurate with the value of the personal information [they] provided in exchange." (*Id*. ¶¶ 44, 52.)

Plaintiffs' allegations of reliance must be rejected because they allege no *factual* support for their *legal* conclusion that they relied on the statement in the Privacy Policy. Plaintiffs merely allege that they "agreed to and relied upon LinkedIn's User Agreement and Privacy Policy, including the material term that 'Personal information you provide will be secured in accordance with industry standard protocols and technology.'" (FAC ¶ 41, 48.) They thus assert a naked legal conclusion—that there was "reliance"—without alleging that, for example, they *read* the Privacy Policy and the particular statement therein or that that statement influenced her decision

in becoming a LinkedIn premium services member. Their allegation of reliance is thus "a legal conclusion couched as a factual allegation." *See Twombly*, 550 U.S. at 555-56 ("courts are not bound to accept as true a legal conclusion couched as a factual allegation" and "a formulaic recitation of the elements of a cause of action will not [survive a motion to dismiss]") (internal quotation marks and citations omitted). Plaintiffs' failure to plead facts to support their allegation of reliance on the statement in the Privacy Policy means that they cannot establish standing through their assertion that they did not receive the "benefit of the bargain."

Even if Plaintiffs had sufficiently alleged reliance, the allegations in the FAC are insufficient to establish that Plaintiffs have Article III standing on a theory that they did not receive the "benefit of the bargain." According to Plaintiffs, the intended purpose of LinkedIn's commitment to use industry standard protocols and technology was "to preserve the integrity and security of [Plaintiffs'] personal information." (*Id.* ¶ 16.) But, as discussed above, the FAC does not plausibly allege that LinkedIn's allegedly substandard encryption protocol for passwords has actually resulted in any misuse of Plaintiffs' personal information by a third party. Plaintiffs' argument is thus akin to the argument recently rejected in *Boysen v. Walgreen Co.*, No. 11-cv-6262, 2012 WL 2953069, at *6 (N.D. Cal. July 19, 2012) (Illston, J.), where plaintiff argued that he was denied the benefit of the bargain by purchasing fruit juice that was marketed as being safe and healthy because it actually contained small amounts of arsenic and lead, and plaintiff asserted that he would not have purchased the fruit juice if he had known that it contained arsenic and lead. The court held that plaintiff did not have Article III standing because he had "failed to allege that he received a 'product that failed to work for its intended purpose or was worth objectively less than what one could reasonabl[y] expect.'" *Id.* (citation omitted); *see also Williams v. Purdue Pharma Co.*, 297 F. Supp. 2d 171 (D.D.C. 2003) (dismissing complaint for lack of standing where plaintiff alleged that defendant deceptively advertised a drug as providing twelve-hour pain relief with little risk of addiction, but where plaintiffs themselves had not alleged that the drug failed to provide them with effective pain relief or that they suffered personal injuries from ingesting the drug). As in *Boysen*, Plaintiffs' allegations that they were denied the "benefit of the bargain" fail to establish Article III standing.

Finally, Plaintiffs allege that the personal information they provided to LinkedIn has economic value or other value the loss of which would constitute injury in fact. (*See, e.g.*, FAC ¶ 35 ("LinkedIn's consumers pay for LinkedIn's products and services both with actual dollars and with their PII."); *id.* ¶ 44 ("[H]ad Plaintiff Szpyrka known of Defendant's substandard security procedures and methods of protecting and storing her PII, she would not have provided her personal and confidential information in exchange for access to Defendant's services. Plaintiff Szpyrka did not receive the benefit of the bargain in that the services provided were not commensurate with the value of the personal information she provided in exchange . . . ."); *id.* ¶ 52 (same for Plaintiff Wright); ¶ 53 ("Plaintiff Wright has suffered damages . . . in the value of her personal data and lost property in the form of her breached and compromised PII.").) These allegations do not help them. Instead, their theory—that the provision of personal information to a defendant has independent economic value or that its loss can constitute an economic loss or injury—has been rejected by numerous courts. *See Low v. LinkedIn Corp.*, No. 11-cv-1468, 2012 WL 2873847, at *12 (N.D. Cal. July 12, 2012) ("theory that [plaintiffs'] personal information has independent economic value is unsupported by decisions of other district courts, which have held that unauthorized collection of personal information does not create an economic loss") (internal citations omitted); *In re iPhone Application Litig.*, No. 11–MD–2250, 2011 WL 4403963, at *5 (N.D. Cal. Sept. 20, 2011) (finding no Article III standing where plaintiffs had not "identified a concrete harm from the alleged collection and tracking of their personal information sufficient to create injury in fact," but instead merely alleged abstract economic injury involving "lost opportunity costs" and "value-for-value exchanges"); *LaCourt v. Specific Media, Inc.*, No. 10-cv-1256, 2011 WL 1661532, at *5 (C.D. Cal. Apr. 28, 2011) (plaintiffs failed to adequately allege injury in fact because they provided no facts showing they "ascribed an economic value" to their personal information, attempted a value-for-value exchange of the information, or were deprived of its value); *Ruiz v. Gap, Inc.*, 540 F. Supp. 2d 1121, 1127-28 (N.D. Cal. 2008) (rejecting contention that unauthorized release of personal information constitutes a loss of property), *aff'd*, 380 Fed. App'x 689 (9th Cir. 2010); *In re Doubleclick, Inc., Privacy Litig.*, 154 F. Supp. 2d 497, 525 (S.D.N.Y. 2001) (unauthorized collection of personal information by a third-party is not

"economic loss"); *In re JetBlue Airways Corp., Privacy Litig.*, 379 F. Supp. 2d 299, 327 (E.D.N.Y. 2005) (disclosure of passenger data to third party in violation of airline's privacy policy had no compensable value); *Dwyer v. Am. Express Co.*, 652 N.E.2d 1351, 1356 (Ill. App. Ct. 1995) (cardholder name has little or no intrinsic value apart from its inclusion on a categorized list; instead, "[d]efendants create value by categorizing and aggregating" the names); *Thompson v. Home Depot, Inc.*, No. 07-cv-1058, 2007 WL 2746603, at *3 (S.D. Cal. Sept. 18, 2007) (finding no loss of money or property under UCL where plaintiff alleged that defendant required customers to provide their personal information as a condition to performing a credit card transaction and used such information for marketing purposes); *In re Facebook Privacy Litig.*, 791 F. Supp. 2d 705, 714 (N.D. Cal. 2011) (plaintiffs received Facebook's services for free and "personal information does not constitute property for purposes of a UCL claim"); *In re Zynga Privacy Litig.*, No. 10-cv-4680, 2011 WL 7479170, at *2 (N.D. Cal. June 15, 2011) (same); *Folgelstrom v. Lamps Plus, Inc.*, 195 Cal. App. 4th 986, 993-994 (2011) (no "intellectual property" interest in home address or economic harm under the UCL for defendant's collection and licensing of plaintiff's personal information; while the information had value to defendant, that "does not mean that its value to plaintiff was diminished in any way").

Because Plaintiffs have failed to allege injury in fact caused by any challenged action of LinkedIn, all of their claims should be dismissed for lack of Article III standing.

B. Plaintiffs Fail to State a Claim Under the UCL (Claim One).

1. Plaintiffs do not have standing under the UCL.

To have standing under the UCL, a plaintiff must have "suffered injury in fact and have lost money or property as a result of the unfair competition." Cal. Bus. & Prof. Code § 17204; *see also Californians for Disability Rights v. Mervyn's, LLC*, 39 Cal. 4th 223, 227 (2006). UCL standing is more restrictive than Article III standing because it is limited to persons who have "lost money or property" "as a result of" the alleged unfair competition. *Kwikset Corp. v. Super. Ct.*, 51 Cal. 4th 310, 322-24 (2011) (the UCL's "narrower" standing requirements include "a loss or deprivation of money or property sufficient to qualify as injury in fact, i.e., *economic injury*").

Plaintiffs have not alleged injury in fact for purposes of UCL standing for the same reasons they have not alleged injury in fact for purposes of Article III standing. (*See supra* § IV.A.)

In addition, Plaintiffs do not, and cannot, meet the "narrower" UCL standing requirements because they do not allege a loss of "money or property" or that such loss was "as a result of" the alleged unfair competition. *First*, as discussed above (*supra* pp. 15-16), Plaintiff Wright's contention that she lost money or property in "the form of the value of their personal data" and lost property "in the form of their breached and compromised PII" (FAC ¶ 76) should be rejected since the mere provision of personal information to another is neither the payment of money nor the payment of property and likewise, the breach or compromise of such personal information does not constitute a loss of property. *See, e.g.*, *Silvaco Data Sys. v. Intel Corp.*, 184 Cal. App. 4th 210, 244 (2010) ("lost money" means that plaintiff has "parted, deliberately or otherwise, with some identifiable sum formerly belonging to him or subject to his control" and "lost property" means that plaintiff has "parted with some particular item of property he formerly owned or possessed; it has ceased to belong to him, or at least has passed beyond his control or ability to retrieve it"); *Facebook*, 791 F. Supp. 2d at 714 (plaintiffs received Facebook's services for free, and "personal information does not constitute property for purposes of a UCL claim"); *Zynga*, 2011 WL 7479170, at *2 (plaintiffs failed to allege that they lost money, and personal information does not constitute property under UCL); *Thompson*, 2007 WL 2746603, at *3 (use of plaintiff's personal information, including a name, for marketing purposes did not confer a property interest to plaintiff under the UCL); *Folgelstrom*, 195 Cal. App. 4th at 993-994 (no "intellectual property" interest in home address or economic harm under the UCL for defendant's collection and licensing of plaintiff's personal information; while the information had value to defendant, that "does not mean that its value to plaintiff was diminished in any way"); *see also supra* pp. 15-16 (citing additional authorities).

Second, regardless of whether Plaintiffs paid a monthly fee or allegedly "paid" by providing personal information, as discussed above (*supra* pp. 9-10, 11-13), Plaintiffs fail to allege that LinkedIn's allegedly substandard encryption protocol for passwords has actually

resulted in any misuse of their personal information by a third party, and thus the FAC does not support a theory that Plaintiffs did not receive the "benefit of the bargain."

Third, as discussed above (*supra* pp. 13-14), Plaintiffs fail to allege facts to support the legal conclusion that they "relied" on the statement in the Privacy Policy when signing up for LinkedIn or subsequently opting for premium services.

Fourth, in addition to being unsupported with factual allegations, Plaintiffs' claim that members rely on the Privacy Policy when signing up for premium services (FAC ¶ 16) does not satisfy the *Twombly*/*Iqbal* plausibility test, particularly in a case like this one. *See Grigsby v. Valve Corp.*, No. 12-cv-0553, 2012 WL 5993755, at *4 (W.D. Wash. Nov. 14, 2012) ("A complex, large-scale case such as a class action should naturally have a higher plausibility threshold than a simpler case.") (citing *Twombly*, 550 U.S. at 557-58). LinkedIn's premium services allow members various additional benefits on top of the regular, free LinkedIn service. Members, for example, gain enhanced communication and visibility services, better search capabilities, and profile management tools. Plaintiffs received all of the LinkedIn benefits they paid for. As Plaintiffs themselves state, as prospective members they "agreed to LinkedIn's User Agreement and Privacy Policy in order to register" with LinkedIn (FAC ¶ 15) and in "creating an account with [LinkedIn]" (FAC ¶¶ 15, 41, 48). Members do not agree to any new User Agreement or Privacy Policy when purchasing upgraded, premium services. Instead, in exchange for the additional services provided by LinkedIn, the upgrading members merely agree to a few new terms related to payment; the remainder of the language is exactly the same as the User Agreement to which they previously agreed when, as prospective members, they initially registered for a LinkedIn account. (*See id.* ¶¶ 15-16; *compare* Heath Decl. Ex. A (User Agreement assented to when initially signing up for free LinkedIn account) *with id.* Ex. C (terms assented to when later upgrading to premium services).) Accordingly, the bargain that members enter into when upgrading to premium services is not based on any promise in the Privacy Policy regarding how LinkedIn will secure their data. Thus, the claim that Plaintiffs would have paid

less for the premium services that they received from LinkedIn if they had known that their password was being secured in unsalted SHA-1 format fails the plausibility requirement.[10]

2. Plaintiffs fail to state a claim under the UCL.

Plaintiffs fail to state a claim under the UCL's "unfair" prong. First, their claim is premised on a theory of deception—i.e., that "LinkedIn willfully and knowingly failed to expend the resources necessary to protect the sensitive data" and "creat[ed] the perception that it followed industry standard protocols" (FAC ¶ 67), and that such "unfair or deceptive practices" (FAC ¶ 75) were "likely to deceive consumers" (FAC ¶ 68) or "mislead the public" (FAC ¶ 71). Accordingly, such a claim is grounded in fraud and must be pled with the particularity required by Federal Rule of Civil Procedure 9(b). *Kearns v. Ford Motor Co.*, 567 F.3d 1120, 1122 (9th Cir. 2009). To adequately plead claims grounded in fraud, Plaintiffs must include particularized allegations that include the "'who, what, when, where, and how' of the misconduct charged." *See Vess v. Ciba-Geigy Corp USA.*, 317 F.3d 1097, 1106 (9th Cir. 2003) (citation omitted). But, as discussed above (*see supra* pp. 13-14), Plaintiffs' allegations consist of mere legal conclusions of "reliance" without any particularized factual allegation concerning whether they actually read the Privacy Policy or the specific statement in question, or the surrounding circumstances of their alleged reliance on that statement. *See Sateriale v. R.J. Reynolds Tobacco Co.*, 697 F.3d 777, 793 (9th Cir. 2012) (where UCL claim sounds in fraud, plaintiffs "are required to prove actual reliance on the allegedly deceptive or misleading statements, and that the misrepresentation was an immediate cause of [their] injury-producing conduct") (citations and internal quotation marks omitted); *Low*, 2012 WL 2873847, at *11 ("[A]lthough the [complaint] describes the terms of

[10] This conclusion is bolstered by the fact that even since the alleged data breach, Szpyrka has *remained a LinkedIn premium services member*. (*See* FAC ¶ 39 ("from December 2011 to the present she has paid $26.95 per month").) Thus, while Szpyrka may allege that she would not have paid as much for premium services if she had known about the way LinkedIn stored member passwords, her own alleged behavior is completely inconsistent with the notion that she believes she was not receiving the benefit of the bargain from LinkedIn's premium services. *See McLaughlin v. Am. Tobacco Co.*, 522 F.3d 215, 226 (2d Cir. 2008) (the fact that some plaintiffs still continued to purchase defendants' light-cigarette packs even after filing the complaint "suggest[ed] the influence of some other motivation" in purchasing the cigarette packs besides the representation that the "light cigarettes" were "healthier").

Defendant's privacy policy in detail, Plaintiffs never allege that they were aware of the privacy policy, let alone saw or read it."). Indeed, while Plaintiffs identify the term in the Privacy Policy, they fail to allege that they actually read it. *Elias v. Hewlett-Packard Co.*, No. 12-cv-0421, 2012 WL 4857822, at *13 n.3 (N.D. Cal. Oct. 11, 2012) (finding that plaintiffs' UCL claim sounding in fraud failed to state a claim because, among other reasons, "Plaintiff does not allege ever seeing any of [Defendants' affirmative misrepresentations] on the website; indeed, he does not even allege that the statements were present on the website at the time of his purchase").[11]

Second, Plaintiffs have not alleged facts showing that LinkedIn acted "unfairly." Although courts are divided on the standard for "unfair" activity under the UCL, Plaintiffs' allegations are insufficient under any definition. California courts have held that to state a claim for an "unfair" business practice under the UCL action,[12] plaintiffs must allege facts establishing (1) substantial consumer injury; (2) that the injury is not outweighed by countervailing benefits to consumers; and (3) that the injury is one that consumers could not reasonably have avoided. *See Camacho v. Auto Club of S. Cal.*, 142 Cal. App. 4th 1394, 1403 (2006). As discussed above (*see supra* §§ IV.A, IV.B.1), Plaintiffs have not pled any injury, let alone a "substantial" one (or, for that matter, an injury that can be "weighed" against countervailing benefits to consumer or not "avoided" by consumers). Furthermore, apart from the lack of injury, Plaintiffs have only included a conclusory statement that the alleged injury is not outweighed by countervailing benefits to consumers. (FAC ¶ 73 (LinkedIn engaged in conduct "the utility of which is outweighed by the gravity of consequences to Plaintiffs").)[13] And Plaintiffs' allegation that

[11] The FAC does not allege violation of the "fraud" prong of the UCL, but even if it did, it would fail because—as discussed herein—it is not alleged with particularity.

[12] In *Cel-Tech Commc'ns, Inc. v. L.A. Cellular Tel. Co.*, 20 Cal. 4th 163, 185-87 (1999), the court reviewed definitions of "unfair" developed by the lower courts and concluded they were "too amorphous and provide[d] too little guidance to courts and businesses." The court adopted a test for competitor actions, but did not decide what test should apply in consumer actions.

[13] Plaintiffs' claim also fails under the alternative test for "unfairness," *see Pinel v. Aurora Loan Servs., LLC*, 814 F. Supp. 2d 930, 940 (N.D. Cal. 2011) ("[a]n unfair business practice under the UCL is 'one that either offends an established public policy or is immoral, unethical, oppressive, unscrupulous, or substantially injurious to consumers'") (citation omitted), since they make only the most conclusory of allegations of how LinkedIn's conduct rises to the "oppressive" or otherwise aggravated levels contemplated by the courts. (FAC ¶ 73 (alleging LinkedIn's "unfair

"[b]ecause defendant maintained control over the database(s) containing Plaintiffs and the Class members' PII, Plaintiffs and the Class could not have reasonably avoided the injuries alleged herein" (FAC ¶ 74) begs the question of what PII Plaintiffs allege was lost.

C. Plaintiffs Fail to State a Claim for Breach of Contract or Breach of Implied Contract (Claims Two, Four, and Seven).

To state a claim for breach of contract, Plaintiffs must plead four elements: "[1] the contract, [2] plaintiffs' performance (or excuse for nonperformance), [3] defendant's breach, and [4] damage to plaintiff therefrom." *Gautier v. Gen. Tel. Co.*, 234 Cal. App. 2d 302, 305 (1965). Damages are essential to the claim, *see First Commercial Mortg. Co. v. Reece*, 89 Cal. App. 4th 731, 745 (2001); *Ruiz v. Gap, Inc.*, 622 F. Supp. 2d 908, 917 (N.D. Cal. 2009) ("Under California law, a breach of a contract claim requires a showing of appreciable and actual damage."), and must be *a result of* the alleged breach, Cal. Civ. Code § 3300 (damages must be "proximately caused" by the breach).

Plaintiffs' breach of contract and implied contract claims should be dismissed because Plaintiffs have not alleged that they have been damaged as a result of LinkedIn's alleged breach of the Privacy Policy. As discussed above (*supra* pp. 15-16), Plaintiff Wright's contention that she suffered injury in "the value of [her] personal data" and lost property "in the form of [her] breached and compromised PII" (FAC ¶ 98) should be rejected; courts have repeatedly rejected the theory that the provision or loss of personal information alone can form the basis for damages.[14] Further, as discussed above (*supra* pp. 9-10, 11-13), this allegation is insufficient

---

conduct was substantially injurious" because LinkedIn knowingly collected fees "paid in part for LinkedIn['s] promise to use industry standard protocols and technology to protect their PII, when in reality, it did not employ such practices").) Plaintiffs fail to allege any injury, let alone a substantial one, and provide no further support for how encryption of passwords using an "unsalted" as opposed to "salted" method (*id.* ¶ 18) meets the aggravated level of "unfair" conduct.

[14] Although not specifically pled within their claims for breach of contract or breach of implied contract, any allegation that Plaintiff Szpyrka and Wright suffered injury by providing personal information to LinkedIn (FAC ¶¶ 44, 52) and not receiving commensurate value in return should be rejected for the same reason that personal information has no independent economic value. (*Supra* pp. 15-16.)

given that Plaintiff Wright does not allege that her password has been used in any way by a third party.[15] Szpyrka, on the other hand, has not alleged that her password was even stolen, let alone decrypted or used. Thus, neither Wright nor Szpyrka has suffered damages "proximately caused" by LinkedIn's breach. *See* Cal. Civ. Code § 3300. And neither can show "appreciable and actual damage." *Ruiz*, 622 F. Supp. 2d at 917.

Plaintiffs' claim for relief in the form of money paid to LinkedIn in exchange for premium services (*see* FAC ¶¶ 43, 51, 84, 98, Prayer for Relief ¶ D) should be rejected because such relief is not available based on their claims as alleged. The return of the money paid to LinkedIn does not constitute legal "damages" resulting from the alleged breach of the Privacy Policy. *See* Cal. Civ. Code § 3300 (damages for breach of contract is "the amount which will compensate the party aggrieved for all the detriment proximately caused thereby, or which, in the ordinary course of things, would be likely to result therefrom"); *see also Coughlin v. Blair*, 41 Cal. 2d 587, 600 (1953) (same). Instead, their request for money paid is—at best—a request for restitution from LinkedIn. *See People v. Martinson*, 188 Cal. App. 3d 894, 900 (1986) (restitution is "restoration of the status quo by the awarding of an amount which would put plaintiff in as good a position as he would have been if no contract had been made and restores to plaintiff value of what he parted with in performing the contract") (internal quotation marks and citation omitted). But restitution can generally be recovered on a contract only in two situations: (1) where the contract was procured by fraud or is otherwise unenforceable, *McBride v. Boughton*, 123 Cal. App. 4th 379, 388 (2004) ("[R]estitution may be awarded in lieu of breach of contract damages when the parties had an express contract, but it was procured by fraud or is unenforceable or ineffective for some reason."); or (2) where defendant's breach is "total" and plaintiff elects to treat the contract as if it were rescinded, *Brown v. Grimes*, 192 Cal. App. 4th 265, 281 (2011) ("A party is entitled to restitution when the contract has failed, such as when it is void, or has been rescinded or '*the consideration has wholly failed*.' Thus, a failure of performance generally gives rise to a claim for restitution of money had and received only when there has been a total breach—i.e., total

[15] And, as discussed above, the FAC does not even clearly allege that Wright's password was decrypted. (*See supra* n.5.)

failure of consideration or repudiation.") (italics in original; citations omitted); *id.* (quoting Perillo, Joseph M., CALAMARI AND PERILLOS HORNBOOK ON CONTRACTS § 15.3 (6th ed. 2009) for the proposition that "[r]estitution is available as a remedy for total breach only, not for a partial breach … the non-breaching party must elect to cancel the contract"). Plaintiffs make *no* such allegations. They do not plead that the contract is unenforceable, whether due to fraud or otherwise. Nor do they plead that there has been a "total" failure of consideration such that the contract must be treated as if it were rescinded. To the contrary, they allege that there was "a valid and enforceable contract between [Plaintiffs] and Defendant." (FAC ¶¶ 80, 94.) Their request for the money paid to LinkedIn is thus unavailable as relief for their breach of contract claim and is an insufficient allegation of the required element of "damages." *First Commercial Mortg.*, 89 Cal. App. 4th at 745 (damages are an essential element to a breach of contract claim). Their breach of contract claim thus fails as a matter of law.

Plaintiffs' claim for breach of implied contract should be dismissed for the same reasons their breach of contract claims should be dismissed since the legal principles applicable here to the breach of contract claims are equally applicable to the breach of implied contract claim. *See* Cal. Civ. Code § 1619 ("A contract is either express or implied."); *id.* § 1621 ("An implied contract is one, the existence and terms of which are manifested by conduct."). Furthermore, their claim for breach of implied contract should also be dismissed since they allege that a "valid and enforceable" express contract exists (FAC ¶¶ 80, 94) which governs the relationship between the parties and addresses any obligations to secure and safeguard Plaintiffs' personal information (FAC ¶¶ 81, 95, 108, 110). *See Roling v. E*Trade Secs., LLC*, 756 F. Supp. 2d 1179, 1189 (N.D. Cal. 2010) ("the existence of an express contract indisputably precludes allegations regarding an implied contract for the same subject matter").

Plaintiffs therefore fail to state any appreciable and actual damage and, accordingly, their breach of contract and breach of implied contract claims must be dismissed.

D. Plaintiffs' "Restitution/Unjust Enrichment" Claims Fail as a Matter of Law (Claims Three and Five).

Plaintiffs' claims for "restitution/unjust enrichment" fail for a number of independent reasons. As an initial matter, several recent California Court of Appeal decisions have made it clear that unjust enrichment does not exist as a stand-alone cause of action under California law. *See Fraley v. Facebook, Inc.*, 830 F. Supp. 2d 785, 814-15 (N.D. Cal. 2011) ("Notwithstanding earlier cases suggesting the existence of a separate, stand-alone cause of action for unjust enrichment, the California Court of Appeals has recently clarified that '[u]njust enrichment is not a cause of action, just a restitution claim.' . . . Thus, Plaintiffs' unjust enrichment claim does not properly state an independent cause of action and must be dismissed.") (quoting *Hill v. Roll Int'l Corp.*, 195 Cal. App. 4th 1295, 1307 (2011) and collecting authorities); *Durell v. Sharp Healthcare*, 183 Cal. App. 4th 1350, 1370 (2010) ("[T]here is no cause of action in California for unjust enrichment."); *Levine v. Blue Shield of Cal.*, 189 Cal. App. 4th 1117, 1138 (2010) (same); *Jogani v. Super. Ct.*, 165 Cal. App. 4th 901, 911 (2008) (same); *McKell v. Wash. Mut., Inc.*, 142 Cal. App. 4th 1457, 1490 (2006) (same); *Melchior v. New Line Prods., Inc.*, 106 Cal. App. 4th 779, 793 (2003) (same); *McBride*, 123 Cal. App. 4th at 387 ("Unjust enrichment is not a cause of action, however, or even a remedy . . . ."). Instead, "unjust enrichment is a basis for obtaining restitution based on quasi-contract or imposition of a constructive trust." *McKell*, 142 Cal. App. 4th at 1490; *see also Melchior*, 106 Cal. App. 4th at 793 ("The phrase 'Unjust Enrichment' does not describe a theory of recovery, but an effect: the result of a failure to make restitution under circumstances where it is equitable to do so. Unjust enrichment is a general principle, underlying various legal doctrines and remedies, rather than a remedy itself.") (citations and internal quotation marks omitted).[16] A claim for unjust enrichment therefore cannot survive unless the court elects to reinterpret the "unjust enrichment" claim as an alternative legal theory that gives

[16] Nor is restitution a cause of action, as these cases make clear. Rather, restitution is a *remedy* that may be awarded when a plaintiff carries the burden of proving a particular cause of action and the requirements for granting a restitutionary remedy are met.

rise to the restitutionary remedy. *See GA Escrow, LLC v. Autonomy Corp., PLC*, No. 08-cv-1784, 2008 WL 4848036, at *7 (N.D. Cal. Nov. 7, 2008).

However, even if "restitution/unjust enrichment" were a stand-alone cause of action, Plaintiffs' claims must still be dismissed because (1) the parties do not dispute the existence of a valid and enforceable contract, rendering Plaintiffs' unjust enrichment claims moot, and (2) Plaintiffs fail to allege a legal theory that would give rise to a restitutionary remedy.

Plaintiffs' restitution/unjust enrichment claims must be dismissed because they do not affirmatively allege the absence of an enforceable agreement. *See Klein v. Chevron U.S.A., Inc.*, 202 Cal. App. 4th 1342, 1389 (2012) ("Although a plaintiff may plead inconsistent claims that allege both the existence of an enforceable agreement and the absence of an enforceable agreement, that is not what occurred here. Instead, plaintiffs' breach of contract claim pleaded the existence of an enforceable agreement and their unjust enrichment claim did not deny the existence or enforceability of that agreement."). As in *Klein*, while Plaintiffs allege that the "members will have no valid contractual relationship with [LinkedIn]" if the contract is found "invalid or unenforceable" (*see* FAC ¶¶ 86, 100), they do not actually plead that the contract is, in fact, invalid or unenforceable. To the contrary, and like the allegations in *Klein*, Plaintiffs allege that there *is* a "valid and enforceable contract." (FAC ¶¶ 80, 94.) In fact, the existence of such a contract is Plaintiffs' core allegation, running as a central theme through the entire FAC—that LinkedIn's Privacy Policy (i.e., the express contract) contains the express term that "[a]ll information that [they] provide [to LinkedIn] will be protected with industry standard protocols and technology" (*id.* ¶ 3) but that "LinkedIn failed to adequately protect user data because it stored passwords in unsalted SHA-1 hashed format" (*id.* ¶ 18). Because Plaintiffs do not make this minimum required allegation denying the existence of the contract, their claim for restitution/unjust enrichment must be rejected as insufficient as a matter of law. *See Allen v. Hylands, Inc.*, No. 12-cv-1150, 2012 WL 1656750, at *5 (C.D. Cal. May 2, 2012) (dismissing unjust enrichment claim and holding that "absent any allegation that Plaintiffs' purchases were not enforceable agreements, Plaintiffs' quasi-contract claims are likewise not viable given Plaintiffs' recourse to warranty-based theories of recovery").

Even if Plaintiffs' allegations could possibly be construed as an affirmative denial of the express contract, their claim for restitution/unjust enrichment must still be dismissed because they have not pled any supporting allegations to sustain the claim. They do not make any allegations as to *how* or *why* the express contract would be invalid or unenforceable such that the remedy for restitution would arise. *See Levine*, 189 Cal. App. 4th at 1138 (affirming the sustaining of demurrer where plaintiffs "have not demonstrated any basis on which they would be entitled to restitution"). Again, as discussed above, where a contract is alleged to exist, as here, restitution can generally be recovered on the contract only in two situations: (1) where the contract was procured by fraud or is otherwise unenforceable, or (2) where defendant's breach is "total" and plaintiff elects to treat the contract as if it were rescinded. (*See supra* pp. 22-23 (citing authorities).) But Plaintiffs do not plead that the contract is unenforceable, whether due to fraud or otherwise. Nor do they plead that there has been a "total" failure of consideration such that the contract must be treated as if it were rescinded. To the contrary, Plaintiffs allege that the User Agreement and Privacy Policy "constitute a valid and enforceable contract between [Plaintiffs] and Defendant." (FAC ¶¶ 80, 94.) Furthermore, any claim for fraud in the inducement must be pled with specificity under Rule 9(b), which Plaintiffs have not done. (*See supra* §§ IV.B.2.)

Accordingly, Plaintiffs' claims for restitution/unjust enrichment must be dismissed.

E. Plaintiffs Fail to State a Claim for Breach of The Implied Covenant of Good Faith and Fair Dealing (Claim Six).

Plaintiffs' breach-of-implied-covenant claim fails for the same reasons that their breach of contract claims fail: they have not alleged damages resulting from the alleged breach. (*See supra* § IV.D); *see also Lyons v. Coxcom*, 718 F. Supp. 2d 1232, 1240 (S.D. Cal. 2009) ("Plaintiff's claim for breach of contract fails, and thus under either California or Georgia law her claim for breach of the implied covenant must also fail.").

This claim should also be dismissed on the independent ground that it is duplicative of the breach of contract claim. Where the allegations in support of a breach-of-implied-covenant claim "do not go beyond the statement of a mere contract breach and, relying on the same alleged acts, simply seek the same damages or other relief already claimed in a companion contract cause of

action, they may be disregarded as superfluous as no additional claim is actually stated." *Careau & Co. v. Sec. Pac. Bus. Credit, Inc.*, 222 Cal. App. 3d 1371, 1395 (1990). Here, the two claims rely on the same allegations—failure to use "industry standard protocols and technology" to encrypt Plaintiffs' passwords (*see* FAC ¶ 15; *see also id.* ¶¶ 18, 83, 97, 110, 113)—and therefore they both should be dismissed. *See In re Zynga Privacy Litig.*, No. 10-cv-04680, Order Granting Def.'s Mot. to Strike & Mot. to Dismiss (ECF No. 85), 8 (N.D. Cal. Nov. 22, 2011) (dismissing implied covenant claim as "superfluous" where it alleged same acts as breach of contract claim).

Finally, Plaintiffs' breach-of-implied-covenant claim does not allege the type of "conscious and deliberate" acts that are required. *Careau*, 222 Cal. App. 3d at 1395 (breach must be "prompted not by an honest mistake, bad judgment or negligence but rather by a conscious and deliberate act"). Plaintiffs' conclusory allegation that LinkedIn "acted consciously and deliberately" (FAC ¶ 112) is unsupported by any fact that could support why or how the alleged acts went beyond "an honest mistake, bad judgment, or negligence" and crossed into the realm of consciously and deliberately attempting to frustrate any common purpose.

F. Plaintiffs Fail to State a Claim for Negligence (Claims Eight and Nine).

The FAC fails to plead facts sufficient to state a negligence claim. "In order to establish liability on a negligence theory, a plaintiff must prove duty, breach, causation, and damages." *Conroy v. Regents of the Univ. of Cal*, 45 Cal. 4th. 1244, 1250 (2009). "Damages must be pleaded and proved as an essential element in a negligence action." *Marenger v. Hartford Accident & Indem. Co.*, 219 Cal. App. 3d 625, 632 (1990); *see also Fields v. Napa Mill. Co.*, 164 Cal. App. 2d 442, 447-48 (1958) ("It is fundamental that a negligent act is not actionable unless it results in injury to another . . . . Nominal damages, to vindicate a technical right, cannot be recovered in a negligence action, where no actual loss has occurred.") (citation omitted). "Under California law, appreciable, nonspeculative, present harm is an essential element of a negligence cause of action." *Ruiz*, 622 F. Supp. 2d at 913.

Plaintiffs have not sufficiently alleged they have been damaged as a result of LinkedIn's failure to encrypt passwords in the format Plaintiffs argue should have been used. As discussed above (*supra* pp. 9-10, 11-13), neither Plaintiff alleges that LinkedIn's allegedly substandard

encryption protocol for passwords actually resulted in any misuse of their personal information by a third party and, accordingly, Plaintiffs' allegations that they did not receive the benefit of the bargain for their monthly fees or for providing "valuable" PII (FAC ¶ 130) should be rejected; and similarly, any claim of damage in that their PII was "compromised" and "exposed" (FAC ¶ 126) is insufficient in the absence of resulting harm or misuse by a third party. Additionally, Plaintiffs' allegations that they suffered damage by providing PII to LinkedIn or that their PII was subject to disclosure (FAC ¶ 130) are insufficient because PII has no value in and of itself. *See, e.g., In re Facebook Privacy Litig.*, No. 10-cv-2389, 2011 WL 6176208, at *5 (N.D. Cal. Nov. 22, 2011) (rejecting theory that plaintiffs' personally identifiable information had value); *see also supra* pp. 15-16 (citing additional authorities). Therefore, Plaintiffs' benefit-of-the-bargain allegations fail to claim any resulting appreciable, non-speculative harm.

Plaintiffs' claims are also barred by the "economic loss rule." Plaintiffs do not claim that they incurred any personal injury or property damage, but instead seek to recover money they paid to LinkedIn on the alleged basis that they did not receive the full benefit of their respective bargains. But in negligence actions, the economic loss rule precludes recovery for damages such as "the difference between price paid and value received, and deviations from standards of quality that have not resulted in property damage or personal injury." *Aas v. Super. Ct.*, 24 Cal. 4th 627, 636 (2000) (superseded by statute on other grounds); *see also Robinson Helicopter Co., Inc. v. Dana Corp.*, 34 Cal. 4th 979, 988 (2004) ("The economic loss rule requires a purchaser to recover in contract for purely economic loss due to disappointed expectations, unless he can demonstrate harm above and beyond a broken contractual promise."). Such claims must be pursued pursuant to contract law, not tort law. *Robinson*, 34 Cal. 4th at 988.

Furthermore, even if Plaintiffs' claims were not barred by the economic loss rule, the bargain that members enter into when signing up for premium services is not tied to how LinkedIn secures their data; rather, the member pays a fee to LinkedIn for certain additional, specified premium services, and the allegation that they would have paid less for the premium services if they had known that their password was being secured in unsalted SHA-1 format fails the plausibility test. (*See supra* pp. 18-19 & n.10.) This conclusion is bolstered by the fact that

Szpyrka has remained a premium services member. (*See* FAC ¶ 39.) Plaintiffs therefore fail to state an appreciable, non-speculative, present injury and their negligence claim must be dismissed.

Plaintiffs similarly fail to state a claim for "negligence *per se*" since that doctrine is "merely an evidentiary doctrine and not an independent cause of action." *People of Cal. v. Kinder Morgan Energy Partners, L.P.*, 569 F. Supp. 2d 1073, 1087 (S.D. Cal. 2008). The negligence *per se* rule operates only to satisfy the "lack of due care" element in a negligence action, not as a cause of action in and of itself. *See Kinney v. CSB Constr., Inc.*, 87 Cal. App. 4th 28, 39 (2001). Thus, pleading negligence *per se* does not relieve Plaintiffs of their burden of alleging resulting damages. *See Sierra-Bay Fed. Land Bank Ass'n v. Super. Ct.*, 227 Cal. App. 3d 318, 333-34 (1991) ("[I]t is the tort of negligence, and not the violation of the statute itself, which entitles a plaintiff to recover civil damages."). Accordingly, all of the arguments above apply equally to Plaintiffs' negligence *per se* claim.

Moreover, Plaintiffs' negligence *per se* claim fails because they have failed to adequately plead a statutory violation. Negligence *per se* creates a presumption of negligence that "arises from the violation of a statute which was enacted to protect a class of persons of which the plaintiff is a member against the type of harm that the plaintiff suffered as a result of the violation." *Greystone Homes, Inc. v. Midtec, Inc.*, 168 Cal. App. 4th 1194, 1226 (2008) (internal quotation and citation omitted). Plaintiffs rely on the UCL violation as support for a finding of negligence *per se*, but because they fail to state a claim under that statute, they fail to plead the lack-of-due-care element.

G. Plaintiffs' Claims Should Be Dismissed With Prejudice.

Plaintiffs' claims should be dismissed with prejudice because—despite numerous original complaints, a Consolidated Class Action Complaint, and a First Amended Consolidated Class Action Complaint—Plaintiffs have failed to put forward any cognizable theory under which they either have been injured in fact or can allege facts sufficient to state a claim. Plaintiffs' First Amended Complaint was drafted in response to LinkedIn's motion to dismiss the Consolidated Class Action Complaint after Plaintiffs had seen LinkedIn's arguments on why that complaint

should be dismissed. *See Zucco Partners, LLC v. Digimarc Corp.*, 552 F.3d 981, 1007 (9th Cir. 2009) ("where the plaintiff has previously been granted leave to amend and has subsequently failed to add the requisite particularity to its claims, '[t]he district court's discretion to deny leave to amend is particularly broad.'") (citation omitted); *Allen v. City of Beverly Hills*, 911 F.2d 367, 373 (9th Cir. 1990) (a "district court's discretion to deny leave to amend is particularly broad where plaintiff has previously amended the complaint") (citation omitted). Given that Plaintiffs' amendments have done nothing to cure the deficiencies LinkedIn identified as to the earlier Consolidated Class Action Complaint, it is clear that any further amendment would thus be futile. *See Steckman v. Hart Brewing, Inc.*, 143 F.3d 1293, 1298 (9th Cir. 1998) (leave to amend should not be granted where amendment would be futile).

V. CONCLUSION

For the foregoing reasons, Plaintiffs' First Amended Complaint should be dismissed with prejudice for lack of standing and for failure to state a claim upon which relief can be granted.

Dated: December 20, 2012

COOLEY LLP

/s/ Matthew D. Brown
Matthew D. Brown

Attorneys for Defendant LinkedIn Corporation

1299157/sf